(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 August 2003 (14.08.2003)

PCT

(10) International Publication Number
WO 03/067850 A1

(51) International Patent Classification[7]: H04L 29/06, G06F 1/00, H04L 9/32

(21) International Application Number: PCT/US03/03622

(22) International Filing Date: 8 February 2003 (08.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/354,930 8 February 2002 (08.02.2002) US

(71) Applicant: INGRIAN NETWORKS, INC. [US/US]; 475 Broadway Street, Redwood City, CA 94063 (US).

(72) Inventors: HILL, Daniel; 3071 Edison Way, Redwood City, CA 94063 (US). FOUNTAIN, Tom; 3071 Edison Way, Redwood City, CA 94063 (US). FRINDELL, Alan; 604 Ranchito Way, Mountain View, CA 94041 (US). MODADUGU, Nagendra; 1670 El Camino Road, #358, Menlo Park, CA 94025 (US).

(74) Agent: MEHRA, Shailesh; Perkins Coie LLP, 101 Jefferson Drive, Menlo Park, CA 94025 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/067850 A1

(54) Title: VERIFYING DIGITAL CONTENT INTEGRITY

(57) Abstract: A system and method for verifying the integrity of digital content in a server environment is described. Content from the server environment, as from a publishing server, is transferred to a content distribution server via a content integrity device. The content integrity device performs cryptographic operations on the content prior to its arrival at the content distribution server. The results of the cryptographic operation are associated and stored with the digital content. Upon receiving a request for the digital content from a source outside of the server environment, the content distribution server identifies and forwards the digital content and results of the associated cryptographic operation to a second integrity device. This device verifies the integrity of the content by comparing the results of similar cryptographic operations performed by the second integrity device with those performed by the first content integrity device.

VERIFYING DIGITAL CONTENT INTEGRITY

Technical Field

The following disclosure relates generally to the field of data security and more particularly to verifying the integrity of content in a server environment.

Background

Various mechanisms exist to enhance the security of digital content associated with networks such as the World Wide Web and the Internet. These mechanisms include the use of passwords, firewalls, access and intrusion control devices, encryption techniques, and others that address the ease of accessing and altering information on the World Wide Web. To protect data during transit, most web sites or server computers use some form of secure protocol such as Secure Socket Layer (SSL).

The use of session keys known only to a client computer and a corresponding web server secures data while it is in transit by uniquely encrypting the data. However, the security of the data before or after the transmission is not guaranteed. While the data resides on the Web server or in computers throughout the server environment, the data is subject to attacks and intrusions from a number of avenues. Web servers have many access points. Data housed on a Web server or computers in a server environment can be accessed by any number of entry means including administrative functions, e-mail, publishing, and diagnostics. Furthermore, backdoors and other vulnerabilities exist that make protecting web content extremely difficult.

As technology has advanced, so has the ability for unwanted intrusions into a company's network. While not all intrusions are malicious in nature, the resulting interruptions frequently result in loss of revenue and damage to reputation. Users demand Internet sites to be available 24 hours per day, 7 days a week. Web site downtime causes immediate sales losses and often damages public confidence longer term. Compounding the nature of competition in e-business, in which alternatives are only a mouse click away, are hackers who often invade and alter web sites as a matter

of pride. Invasions into a web server can corrupt web sites, defacing the sites aesthetically and/or conveying bogus information. Such invasions often cost revenue and good will. Encountering false data is an experience that can mean a permanent loss of a customer. Companies invest intensively to provide a highly available and positive user experience. It is therefore necessary to protect digital content while the content is in transit and while the content is stored. A company must be able to rely on the integrity of the information being posted on the company's web server.

The challenge has been to arrive at a balance between security and accessibility. It is easier to build an impenetrable safe than it is to build a secure repository of information that delivers requested data reliably. It is also desirable to safeguard against intrusion in a manner that is transparent to the server environment, the web server, and the web user. These and other challenges are addressed in the following disclosure.

Brief Description of the Drawings

Figure 1 is a block diagram showing one embodiment of a system architecture for verifying content integrity.

Figure 2 is a block diagram showing one embodiment of a hardware architecture for a content integrity device.

Figure 3 is a block diagram showing one embodiment of a software architecture for a content integrity device.

Figure 4 is a flow diagram of one embodiment of a method for verifying content integrity using cryptographic operations.

Figure 5 is a flow diagram of one embodiment of a method for verifying content integrity using digital signatures.

Figure 6 is a flow diagram of one embodiment of a method for verifying content integrity using encryption and digital signatures.

Summary of the Invention

Systems and methods for ensuring the integrity of digital content are described. In embodiments of the invention, the integrity of digital content, as it is transmitted from one computing environment to another computing environment via a communications network, is verified by comparing the results of cryptographic operations performed on the content. In particular, a first cryptographic operation may be performed on digital content, upon which the content may be made available for transmission over the communications network. In some embodiments of the invention, content may be stored for future distribution after the performance of the first cryptographic operation. Prior to the release of the digital content, a second, corresponding cryptographic operation may be performed upon the digital content. As a precondition to releasing the content to a requestor, the integrity of the content is verified to ensure it has not been altered. In embodiments of the invention, these verification protocols can be performed by use of a content integrity device; this enables the operations to be performed transparently, without necessitating any modifications to existing software architectures.

In embodiments of the invention, two content integrity devices may be coupled to a content distribution device in communication with the external network; in some such embodiments, the content distribution device is a content distribution server. Digital content which is intended for publishing is intercepted by one of the content integrity devices as the content travels to the content distribution server. Upon arrival at the first content integrity device, the device performs a cryptographic operation such as a digital signature of the content. Once the digital signature has been created, the digital content and signature are passed to the content distribution server. Upon receiving a request for the digital content from outside the server environment, the content distribution server identifies the requested digital content and passes the digital content and its associated signature to a second content integrity device.

The second content integrity device executes the corresponding cryptographic operations performed by the first content integrity device upon the digital content. In some embodiments of the invention, the signature prepared by the second content integrity device is compared to the original in order to verify the content. If, and only if, the digital content is verified, the content integrity device concludes that the integrity of

the digital content is intact and, accordingly, forwards the digital content to the requester outside of the server environment.

Another aspect of the invention includes ensuring the privacy of the digital content while the content resides on a content distribution server, storage medium, or isolated network. Content released for publication by one computing environment is intercepted by a content integrity device. The content integrity device performs cryptographic operations on the content, operations which may include, but are not limited to, the creation of a digital signature. Other cryptographic operations may which may also be performed include encryption and compression operations. In some such embodiments, content which has been encrypted, along with associated digital signatures are passed to a content distribution server where the encrypted content and signature reside until requested by a user outside of the server environment. Upon receiving an external request for the digital content, the content distribution server identifies the encrypted content as the content requested by the user and forwards the encrypted content and associated signature to another content integrity device. The second content integrity device, proceeds to (1) decrypt the content and (2) verify the integrity of the decrypted content. The decrypted digital content is released to the requesting user only after verifying the digital signature.

Other embodiments of the invention include caching the content on a content integrity device so that if altered content is discovered, previously verified content can be forwarded to the requesting user without having to reacquire content from its source. Other aspects of the content integrity device include other cryptographic operations and combinations of cryptographic operations to verify the integrity of the content and ensure the security of the content while residing on the content distribution server. These and other embodiments are described in greater detail herein.

Detailed Description of the Illustrated Embodiments

A. Overview

The invention described herein includes systems and methods for securing and verifying the integrity of digital content. In embodiments of the invention, digital content produced within a secure environment may be conveyed to an intermediate device, such as a publishing system, and subsequently made available for access by users

external to the secure environment. In some such embodiments, digital content with is ready for publishing may be forwarded to a content distribution device, such as a web server, via a device which verifies the integrity of the content. Upon receiving the content from the secure, authorized source, the content integrity device performs one or more cryptographic operations on the content, and subsequently makes it assessable to users outside of the secure environment. In embodiments of the invention, when the content distribution device receives an external request for the content, the content is identified and forwarded to a second content integrity device. This second device performs one or more cryptographic operations, such as to examine the content by verifying the associated digital signature performed by the first content integrity device.

In embodiments of the invention, content integrity is verified by a dedicated content integrity device, which is separate from the devices which house the digital content prior to its external publication. In such embodiments, the content integrity devices are coupled to the remaining devices, such as the content dispersal systems and data networks, in a manner that obviates modification to the remaining devices. This enables web site operators or other managers of digital content to ensure the integrity of digital content transparently, without altering current software or modifying existing hardware on their systems.

B. Network Architecture of the Content Integrity System

A network architecture 100 for verifying content integrity is illustrated in Figure 1. The system 100 includes two content integrity devices 102 104. A first content integrity device 102 is coupled among a publishing system 106 and a content distribution server 110. The publishing system 106 may be further coupled to one or more server computers 112. The intranet established by the publishing system and server computers 112 is, for purposes of this discussion, isolated from outside intervention and can be considered a secure environment. The second content integrity device 104 is coupled among the content distribution server 110 and a network 120, such as the Internet or an intranet, which is in turn coupled to several other computers 130 from which content requests may originate; by way of non-limiting example, the requestors may client programs such as web browsers. The requestors 130 can each possess software for accessing network resources, such as, by way of non-limiting example, a

web browser that when directed by a user requests content from the content distribution server. The protocol for exchange and transport of this information can be one of any protocols known to one skilled in the relevant art and includes but is not limited to HyperText Transmission Protocol (HTTP), File Transfer Protocol (FTP), HyperText Transmission Protocol Secure (HTTPS), Common Internet File System (CIFS), and Network File Systems (NFS). Other suitable protocols shall be apparent to those skilled in the art.

In one embodiment of the claimed invention, content developed on the server computers 112 is communicated to the publishing system 106 and passed to the content distribution server 110 via the first content integrity device 102. The first content integrity device 102 generates a first digital signature and digitally signs the content before the content reaches the web server 110. Upon receiving a request for the content from a client computer 130 via network 120, the content is passed from the content distribution server 110 to the second content integrity device 104 where the digital signature is verified. If the content is successfully verified, the content is released to the requesting client computer 130. If the content is not verified, its release is blocked, preventing unauthorized or modified content to be released. In an embodiment of the claimed invention, the content integrity device 104 stores a trusted version of the digital content. This cache may be updated either periodically or each time content is verified prior to transmittal. If the verification process fails, the trusted, cached content can be forwarded to the requesting user in place of the content provided by the content distribution server. In some embodiments of the invention, logs may be maintained which record verification failures. Other responses undertaken in case the content integrity is comprised shall be apparent to those skilled in the art.

The functionality provided by the content integrity device 102 and 104 can be hosted on dedicated network appliances as shown in **Figure 1**, but is not so limited. The content integrity functionality can also be performed by, or distributed among, any combination of the publishing systems 106 and 112, numerous client processing devices and browsers 130 coupled to the network 120, and any of the associated network components. Typically each content integrity device can include at least one processor capable of executing computer executable instructions and at least one storage medium for retention of data and software. In some embodiments of the invention, protection and verification operations can be performed on a single physical

device. Many hardware and/or network architectures which support the content integrity functions will be apparent to those skilled in the art.

The cryptographic operations which may be performed by a content integrity device are multifarious. Encryption operations may be symmetric, such as, by way of non-limiting example, any of the variants of the Data Encryption Standard (DES). Alternatively, asymmetric encryption may be employed, such as, by way of non-limiting example, public-private key algorithms, such as any of the variants of Rivest-Shamir-Ableson (RSA), Pretty Good Privacy (PGP), or other examples which will be apparent to those skilled in the art. The cryptographic operations may include one-way functions, such as one-way hash functions. These one way hash functions may include, by way of non-limiting example, any of the variants of Secure Hash Algorithm (SHA), Message Authentication Code (MAC), and a Message Digest (MD) functions. In embodiments of the invention, a content integrity device may perform multiple encryption functions on digital content. These and other permutations of cryptographic functions in the invention shall be apparent to those skilled in the art.

C. Hardware Architectures of the Content Integrity System

Figure 2 illustrates a hardware architecture 200 for verifying the integrity of digital content. The hardware architecture 200 includes at least one processor 208, a memory system 210, and I/O. Inherent to the architecture 200 is a system bus 206 that operatively couples the various components together. The processing unit may be any logic processing unit, such as one or more central processing units (CPUs), digital signal processors (DSPs), application-specific integrated circuits (ASIC), etc. Unless described otherwise, the construction and operation of the various blocks shown in **Figure 2** are of conventional design. As a result, such blocks need not be described in further detail herein, as they will be readily understood by one skilled in the relevant art.

The operating system 202 contains the basic routines that help transfer information amongst the elements within the architecture 200. In non-limiting embodiments of the invention, the operating system is based on a version of the Linux operating system. The system bus 206 can employ any know bus structures or architectures including a memory bus with memory controller, a peripheral bus, and a local bus. The memory 210 includes read-only memory (ROM) and random access

memory (RAM). The input / output system 216 contains basic routines that help transfer information between elements with the content integrity device. Non-limiting examples of input / output 216 include various forms of Ethernet. The content integrity device can also include secondary storage media, non-limiting examples of which include a hard disk drive for reading from and writing to a hard disk, and an optical disk drive and a magnetic disk drive for reading from and writing to removable optical disks and magnetic disks, respectively. The optical disk can be a CD-ROM, while the magnetic disk can be a magnetic floppy disk. The hard disk drive, optical disk drive and magnetic disk drive communicate with the processing unit 208 via the bus 206. The hard disk drive, optical disk drive and magnetic disk drive may include interfaces or controllers coupled between such drives and the bus 206, as is known by those skilled in the art. The drives and their associated computer-readable media, provide nonvolatile storage of computer readable instructions, data structures, program modules and other data for the content integrity device. Those skilled in the relevant art will appreciate that other types of computer-readable media that can store data accessible by a processor may be employed, such as magnetic cassettes, flash memory cards, digital video disks ("DVD"), Bernoulli cartridges, RAMs, ROMs, smart cards, etc.

Program modules, such as an operating system can be stored in the system memory 210 one or more application programs, other programs or modules, and program data. In embodiments of the invention, the system memory 210 may also include software for permitting the content integrity device to access and exchange data with web sites in the World Wide Web of the Internet.

In one embodiment the system memory 210 stores private and public keys that enable the processing unit 208 to create digital signatures of content received through the input and output ports 216. Furthermore, various algorithms and other computer cryptographic executable codes are retained in the system memory 210 for the encryption and decryption of the digital content. The operating system 202 can also direct the caching of the digital content in both the encrypted and clear text state as well as associating a digital signature generated in the content integrity device with a particular piece of digital content.

A further aspect of the content integrity device is the inclusion of a hardware security module 220 with a smart card. The hardware security module 220 comprises a

tamper resistant device that stores private keys in a secure format. The private keys are encrypted using a separate group key known to a select, predefined group of ancillary network devices. This encrypted group of keys can be transported between the various devices using a smart card. The smart card can also be used to back up the encrypted key data. As the data contained on the smart cards is encrypted with a separate key, the encrypted group of private keys can only be accessed by one of the devices in the predefined group.

Another aspect of the hardware security module is a protocol that supports "k out of n" secret sharing of the separate group key. Such a protocol enhances security by requiring each device to use multiple smart cards for backing up and restoring the private keys. For example, if the private key information is distributed across a group of five smart cards (n=5), preferences can be established requiring three smart cards (k=3) be inserted into a smart card reader before the group data can be accessed. Any attempt to access the data with less than three smart cards will fail. Using a "k out of n" schema ensures data security. If a single card is stolen, misplaced or unaccounted for, a unauthorized user of the card will not be able to access the key data stored on the hardware security module.

D. Software Architecture of the Content Integrity System

Figure 3 shows one embodiment of a software architecture 300 for verifying the integrity of digital content by use of a content integrity device. The architecture 300 includes a caching engine 315, a content identification engine 320, a cryptographic engine 325, a digital signature engine 330, and a process manger 332. As content is received, the process manager 332 uses the digital signature engine 330 and cryptographic engine 325 to perform cryptographic operations on the content. Once completed, the content may optionally be cached using the caching engine 315 for subsequent access and dispersal. In addition to directing cryptographic operations on the content, the process manager 332 uses the content identification engine 320 to associate the content with the digital signature and encrypted data. In one embodiment, the cryptographic engine 325 may embed a numerical representation, such as a digital signature, in the content itself. In other embodiments the numerical representation may or may not be part of the content. Upon receiving a request for the content, the process manager 332, using the content identification engine 320,

identifies and retrieves the content and associated signatures from the cache for dispersal.

In the embodiment shown in **Figure 3**, the process manger 332 manages content received from a server environment 340 that includes a publishing system 350 and other server computers 360. The process manager 332 conveys the content to entities outside the server environment such as a content distribution server 375 and a network 385 such as the Internet. While this embodiment illustrates the software architecture 300 of a content integrity device which is positioned between a server environment 340 and a content distribution server 375, in alternate embodiments an identical software architecture 300 may be placed between the content distribution server 375 and a network 385 to facilitate the verification of the content's integrity as a condition to its distribution over the network 385.

E. Integrity Verification Process

The invention supports several techniques for verifying the integrity of digital content. A method 400 for verifying the integrity of content in a network environment used in embodiments of the invention is illustrated in the flow diagram of Figure 4. Content is published 405 and intercepted by a content integrity device. The content integrity device performs at least one cryptographic operation on the content 410. These operations can include encryption operations, decryption operations, hash operations, keyed hash operations, keyed hash verifications, digital signatures, signature verification, checksums, and other like operations known to those skilled in the relevant art.

Once the desired cryptographic operation has been completed 410, the content is transferred 415, to a content distribution server, along with any associated result from the cryptographic operation, for dissemination over the Internet or like network. The content remains on the content distribution server until an updated version is received from the publishing server. By way of non-limiting example, a client computer may request content from a web page resident on the content distribution server. The content distribution server 420 receives the request for the content and identifies the desired object with the appropriate embedded objects to send. As the content is directed to the client's IP address, the content is intercepted 425 by the second content integrity device.

The second content integrity device performs additional cryptographic operations on the content. Before the content is released to requests originating outside the system, the signature is verified 435. If the verification succeeds, indicating that the content has not been altered, the content integrity device releases the content 440 to the requesting client.

Figure 5 depicts a flow diagram for verifying content integrity 500 by use of digital signatures. Content is received at the first integrity device from a trusted source such as the publishing server 505. Transparent to the publishing server and the content distribution server, the content integrity device creates a digital signature 510. The digital signature can be created using various algorithms known to one skilled in the relevant art. The digital signature of the content is formed in one embodiment by using secret information such as a private key which can be later verified by using public information such as a public key. Other algorithms which may be used to create the digital signature include, but are not limited to one way hashing, keyed hashes such as Keyed Hash Message Authentication Code (HMAC), timestamps, and other techniques that will be apparent to those skilled in the art. Once signed, the digital signature is associated 515 with the content and then transferred to the content distribution server, or other storage medium 520.

In embodiments of the invention, the content remains on the content distribution server until it is either requested by a client or replaced by the publishing server 525. Upon receipt of the request, the appropriate content is identified 530 and ultimately forwarded for integrity verification 535.

The content and the associated signature arrive at the second integrity device where the signature is verified 540. As the algorithms and keys used correspond to the original signature, the signature verification will be successful if the content has not been altered. Likewise the signature verification will fail if false data has been placed on the content distribution server lacking the proper signature. If the signatures are verified 545, the content is released 550 to the requestor. In an alternative embodiment, the content integrity device maintains a cache of the verified content. Upon detecting a discrepancy in the digital signatures, the content integrity device releases the cached content and alerts the network manager of the presence of false data 560. Various other protocols in response to a verification failure can be established that are aligned with the use of the methodology and techniques for

content integrity verification described herein; these protocols shall be apparent to those skilled in the art.

An alternative method for verifying the integrity of digital content is shown in the flow diagram of **Figure 6**. Continuing with the theme of ensuring the integrity of the content prior to its dispersal, this method 600 also protects the privacy of the content as it rests on the content distribution server. As described herein, content is published by the publishing server 605 to a first integrity device. Upon arrival, a digital signature of the content is formed 610 using methodology described herein and known to one skilled in the relevant art. The content is subsequently encrypted 615 using a non-limiting algorithm such as Data Encryption Standard (DES), Rivest Shamir Adleman (RSA), or another cipher commonly known to one skilled in the relevant art. In an alternative embodiment, the content is signed using a private key and encrypted using a distinct public key.

The encrypted content is associated 620 with the digital signature and transferred 625 to the content distribution server. The content and digital signature reside on the content distribution server in an encrypted state until updated by new authorized data. The content remains encrypted until a request for the content 630 is received from a requestor. Upon receiving the request, the content distribution server 635 identifies the content and associated signature. The encrypted content and signature are then forwarded 640 to a second content integrity.

The second content integrity device decrypts the content 645 using, in one embodiment, the corresponding private key of the public/private key pair. With the content decrypted, the digital signature is verified. In one embodiment, verifying the digital signature includes using a public key corresponding to the public/private key pair utilized by the first content integrity device. Other techniques for verifying integrity readily known to those skilled in the relevant art can also be used without affecting the functionality of the invention. Having verified 655 the digital signature, the decrypted content is released 660 to the Internet and ultimately to the requestor. In embodiments of the invention, slightly different operations may be used for the encryption and the signatures.

The system and methodology described herein protects the content on a content distribution server from being stolen and altered by unauthorized users. It further verifies that the content being served to the Internet from a content distribution server is

the content that was intended to be published to the content distribution server. The content is signed as it is being published to the content distribution server. If the signature associated with the content upon transmission from the content distribution server is different from the one when the content was initially published, the transmission is blocked ensuring the client is not exposed to false or misleading data.

Alternative Embodiments

Though many of the embodiments described herein involve the deployment of two content integrity devices, many alternative embodiments shall be apparent to those skilled in the art. For instance, the verification procedures may be performed on a single device. By way of non-limiting example, a single content integrity device may include separate process which perform an initial digital signature on digital content, and then, prior to release by a content distribution server, verify the integrity of the digital content by performing and comparing a second digital signature on the content. In some embodiments of the invention, the digital content device may itself be incorporated into a content distribution server, or may comprise discrete processes within a content distribution server. In some embodiments, the encryption and verification processes described infra may be at least partially performed on line cards within networking devices. Additionally, a content integrity device may perform multiple cryptographic operations on digital content.

Those skilled in the relevant art will appreciate that the routines and other functions and methods described herein can be preformed by or distributed among any of the components described herein. While many of the embodiments are shown and described as being implemented in hardware (e.g. one or more devices designed specifically for a task), such embodiments could equally be implemented in software and be performed by one or more processors. Such software can be stored on any suitable computer-readable medium, such as micro-code stored in a semiconductor chip, on a computer-readable disk, or downloaded from a server and stored locally at a client. The embodiments described herein are for illustrative purposes only; many equivalents and alternatives shall be apparent to those skilled in the art.

CLAIMS

1. A method for verifying integrity of digital content, the method comprising:

computing a first one or more cryptographic operations on the digital content;

upon a request for the digital content, performing a second one or more cryptographic operations on the digital content, the second one or more cryptographic operations including an inversion of the first one or more cryptographic operations;

releasing the digital content in response to the request immediately after performing the second one or more cryptographic operations.

2. The method of claim 1, wherein the first one or more cryptographic operations includes an encryption of the digital content, and the second one or more cryptographic operations includes a corresponding decryption of the digital content.

3. The method of claim 2 wherein the encryption and corresponding decryption are symmetric operations based on a private key.

4. The method of claim 3, wherein the encryption and decryption are based on Data Encryption Standard (DES).

5. The method of claim 2, wherein the encryption is based on a public key, and the decryption is based on a corresponding private key.

6. The method of claim 5, wherein the encryption and corresponding decryption are RSA operations.

7. A method for verifying integrity of digital content, the method comprising:

computing a first one or more cryptographic operations on the digital content;

upon a request for the digital content, performing a second one or more cryptographic operations on the digital content;

comparing a result of the second one or more cryptographic operations with at least one of the digital content and a result of the first one or more cryptographic operations;

releasing the digital content in response to the request if and only if the comparing the result of the first and second one or more cryptographic operations is successful.

8. The method of claim 7, wherein the first one or more cryptographic operations and second one or more cryptographic operations are identical operations.

9. The method of claim 7, wherein the first and second one or more cryptographic operations include one way hash functions.

10. The method of claim 9, wherein the one way hash functions include one or more of Secure Hash Algorithm (SHA), a Message Authentication Code (MAC), a Message Digest (MD) function.

11. The method of claim 10, wherein the MAC is HMAC.

12. The method of claim 10, wherein the MD function is one of MD-2, MD-3, MD-4, MD-5.

13. The method of claim 8, wherein the first and second one or more cryptographic operations comprise, respectively, a first digital signature and a second digital signature.

14. The method of claim 13, wherein the first and second digital signatures are performed by use of a single private key.

15. The method of claim 13, further comprising:

prior to computing the first digital signature, receiving the digital content from a trusted source.

16. The method of claim 17, wherein the trusted source is a secure local network.

17. The method of claim 16, wherein the request for the digital content arrives from an network external to the secure local network.

18. The method of claim 17, wherein the network external to the local network is an internetwork.

19. The method of claim 13, further comprising:

if the first and second signatures do not agree, releasing a previously cached version of the digital content in response to the request.

20. The method of claim 13 further comprising:

if the first and second signatures do not agree, logging a corresponding record in a database of anomalies.

21. The method of claim 13, further comprising:

If the first and second signatures do not agree, denying the request for the digital content.

22. The method of claim 13, further comprising:

after first computing the first digital signature, encrypting the digital content.

23. The method of claim 22, further comprising:

prior to performing the second digital signature, decrypting the digital content.

24. A computer network system for delivering digital content to an external network, wherein in the external network is in communication with the computer network system via at least one content server, the computer network system comprising:

one or more publishing servers for generating and storing digital content, wherein the one or more publishing servers are isolated from the external network;

a first content integrity device for performing and verifying cryptographic operations, such that the content integrity device is coupled to the one or more publishing servers and to the external access device;

a second content integrity device for performing and verifying cryptographic operations, the second content integrity device coupled to the external access device and the external network;

wherein the first content integrity device is configured to intercept digital content forwarded by the one or more publishing servers to the at least one content server, such that the first content integrity generates a cryptographic operation for the digital content, and the second content integrity device is configured to authorize external release of the digital content by the at least one content server, only after verification of the cryptographic operation.

25. The computer network system of claim 24, wherein the external network in an internetwork.

26. The computer network system of claim 24, wherein the digital content is encoded in at least one markup language.

27. The computer network system of claim 24, wherein the at least one markup language is one or more of HTML, XML, SGML.

28. The computer network system of claim 24, wherein the at least one content server includes a web server.

29. The computer network system of claim 24, wherein the digital content includes a PDF file.

30. The computer network system of claim 24, wherein the digital content includes ASCII text.

31. The computer network system of claim 24, wherein a private key is stored in a secure format on the first and second content integrity devices.

32. The computer network system of claim 31, wherein the private key is encrypted in the first and second content integrity devices.

33. The computer network system of claim 32, wherein the private key is encrypted in the first and second devices using a separate group key, such that the separate group key is known to the first and second content integrity devices.

34. The computer network system of claim 33, wherein the first and second content integrity devices each include a smart card port, such that the private key can be received securely by one or more smart cards via the smart card port.

35. The computer network system of claim 34, wherein the private key can be received by use of any k of n smart cards, wherein $k < n$.

36. The computer network system of claim 34, wherein the one or more smart cards includes three or more smart cards, such that the private key is distributed amongst the three or more smart cards, and the first and second content integrity devices read the private key from a plurality of the three or more smart cards.

37. The computer network system of claim 24, wherein the first content integrity device and the one or more publishing servers are coupled via a local area network.

38. The computer network system of claim 37, wherein the second content integrity device and the at least one content server are coupled via a local area network connection.

39. The computer network system of claim 38, wherein the second content integrity device is operable to record each failure in verification of the digital signature.

40. The computer network system of claim 24, wherein the first content integrity device is operable to encrypt the digital content with a private key.

41. The computer network system of claim 40, wherein the second content integrity device stores a public key corresponding to the private key, such that the second content integrity device is operable to decrypt the digital content with the public key.

42. A computer system for verifying the integrity of digital content, wherein the digital content is generated in a secure environment, and is intended for external release, the computer system comprising:

at least one processing device;

a first one or more daemon processes, for intercepting the digital content prior to external release, the first one or more daemon processes operable on the at least one processing device;

a second one or more daemon processes for receiving external requests for the digital content, the second one or more daemon processes operable on the at least one processing device;

a first one or more cryptographic processes for performing a first cryptographic operation on the digital content prior to the receiving external requests for the digital content, the first one or more cryptographic processes operable on the at least one processing device;

a second one or more cryptographic processes executing for performing a second cryptographic operation on the digital content after receiving the external requests for the digital content, the second one or more cryptographic processes resident on the at least one processing device;

one or more verification processes on the computer system for verifying and authorizing release of the digital content, after comparison of the first and second digital signatures, the one or more verification processes resident on the at least one processing device.

43. The computer system of claim 42, wherein the digital content is at least partially encoded in one or more markup languages.

44. The computer system of claim 43, wherein the one or more markup languages includes Hyper Text Markup Language (HTML).

45. The computer system of claim 44, wherein the one or more daemon processes for receiving external requests includes an Hyper Text Transfer Protocol daemon (HTTP).

46. The computer system of claim 46, wherein the HTTP daemon is resident on a dedicated HTTP server.

47. The computer system of claim 44, wherein the one or more daemon processes for receiving external requests includes an Hyper Text Transfer Protocol over SSL (HTTPS) daemon.

48. The computer system of claim 47, wherein the HTTPS daemon is resident on a dedicated HTTPS server.

49. The computer system of claim 43, wherein the one or more markup languages includes eXtensible Markup Language (XML) and Standard Generalized Markup Language (SGML).

50. The computer system of claim 42, wherein the first one or more cryptographic processes are executed at least partially on a dedicated encryption offload processor.

51. The computer system of claim 42, wherein the second one or more cryptographic processes are executed at least partially on a dedicated encryption offload processor.

52. The computer system of claim 42, wherein the first one or more cryptographic processes and second one or more cryptographic processes are at least partially executed on a single server device.

53. The computer system of claim 52, wherein the one or more daemon processes for intercepting the digital content prior to external release and the one or more daemon processes for receiving external requests for the digital content are also performed on the single server device.

54. The computer system of claim 53, wherein the single server device comprises a web server.

55. The computer system of claim 53, further including:
one or more processes for encrypting the digital content.

56. The computer system of claim 55, wherein the one or more processes for encrypting the digital content encrypt the digital content by use of a private key.

57. The computer system of claim 55, wherein the one or more processes for encrypting the digital content are resident on the single server device.

58. The computer system of claim 42, wherein the at least one processing device includes an accelerator card for accelerating the first one or more cryptographic processes.

59. The computer system of claim 58, wherein the at least one processing device includes an accelerator card for accelerating the first one or more cryptographic processes.

60. A method for verifying the integrity of digital content stored initially in a server environment, the method comprising:
signing the digital content using a private key forming a first signature;
associating the digital content with the first signature;

transferring the digital content and the first signature to an external access server, wherein the external access server is in direct communication with at least one network external to the server environment;

after associating the digital content with the first signature, receiving an external request for the digital content at the external access server;

in response to the external request, signing the digital content with the private key to form a second digital signature for the content;

comparing the first signature and the second signature;

if the first and second signatures agree, releasing the digital content from the external access server via the one or more external networks.

61. The method of claim 60, wherein the signing the first digital signature is performed in at least partially in a first dedicated content integrity server, the first content integrity server coupled locally to the external access server.

62. The method of claim 61, wherein the second digital signature is generated in a second dedicated content integrity server, which is locally coupled to the external access server.

63. The method of claim 60, wherein the external access server is a web server.

64. The method of claim 63, wherein the digital content is at least partially encoded in a markup language.

65. The method of claim 64, wherein the markup language is one or more of HTML, SGML, XML.

66. The method of claim 63, wherein the external request is an http request.

67. The method of claim 60 wherein the one or more external networks include an internetwork.

68. The method of claim 60, wherein the first and second digital signatures are generated at the external access server.

69. The method of claim 60, further comprising:

after signing the digital content using the private key to forming the first signature, encrypting the digital content.

70. The method of claim 69, further comprising:

prior to forming the second digital signature, decrypting the digital content.

71. A method for verifying the integrity of digital content stored in a server environment, the method, comprising:

signing the digital content using a private key forming a first signature;

associating the digital content with the first signature;

transferring the digital content and the first signature to an external access server, wherein the external access server is in direct communication with at least one network external to the server environment;

after associating the digital content with the first signature, receiving an external request for the digital content at the external access server;

in response to the external request, signing the digital content with the private key to form a second digital signature for the content;

comparing the first signature and the second signature;

if the first and second signatures do not match,

logging an entry in a database of integrity failures, and

barring external release of the digital content.

72. A method for verifying the integrity of digital content stored in a server environment, the method, comprising:

signing the digital content using a private key forming a first signature;

associating the digital content with the first signature;

transferring the digital content and the first signature to an external access server, wherein the external access server is in direct communication with at least one network external to the server environment;

after associating the digital content with the first signature, receiving an external request for the digital content at the external access server;

in response to the external request, signing the digital content with the private key to form a second digital signature for the content;

comparing the first signature and the second signature;

if the first and second signatures do not match, releasing a previously cached version of the digital content from the external access server.

73. The method of claim 72 wherein the method for verifying the integrity of digital content stored in a server environment, the method, comprising:

signing the digital content using a private key forming a first signature;

associating the digital content with the first signature.

74. A system for verifying the integrity of digital content in a server environment, the system comprising:

at least one web server coupled among two or more network appliances, wherein a first of the two or more network appliances includes

means for receiving the digital content from the server environment,

means for creating a cryptographic transformation of the digital content, and

means for transferring the digital content to the web server, and

wherein a second of the two or more network appliances includes

means for receiving the digital content from the web server, and

means for verifying the digital content before releasing the digital content outside of the server environment.

75. An electromagnetic medium containing executable instructions which, when executed in a processing system, verifies the integrity of digital content by:

identifying the digital content and an associated first signature at a server upon receiving a request from a party outside of the server environment for the digital content;

transferring the digital content and the associated first signature to a processor;

signing the digital content forming a second signature;

verifying successfully the integrity of the digital content; and

releasing the digital content to the party outside of the server environment.

76. A computer readable medium containing executable instructions which, when executed in a processing system, verifies integrity of digital content by:

identifying the digital content and an associated first signature at a server upon receiving a request from a party outside of the server environment for the digital content;

transferring the digital content and the associated first signature to a processor;

signing the digital content forming a second signature;

verifying successfully the integrity of the digital content; and

releasing the digital content to the party outside of the server environment.

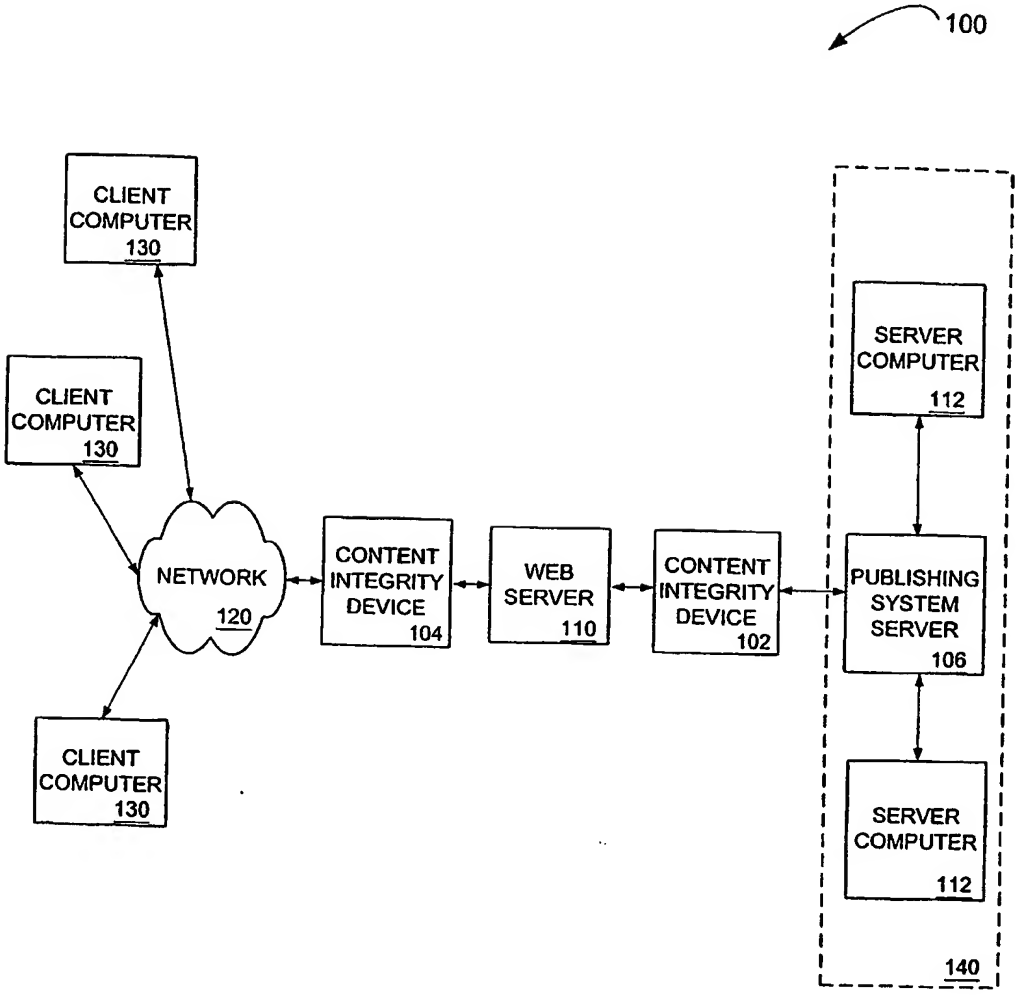
100
CLIENT COMPUTER 130
CLIENT COMPUTER 130
CLIENT COMPUTER 130
NETWORK 120
CONTENT INTEGRITY DEVICE 104
WEB SERVER 110
CONTENT INTEGRITY DEVICE 102
SERVER COMPUTER 112
PUBLISHING SYSTEM SERVER 106
SERVER COMPUTER 112
140

FIG. 1

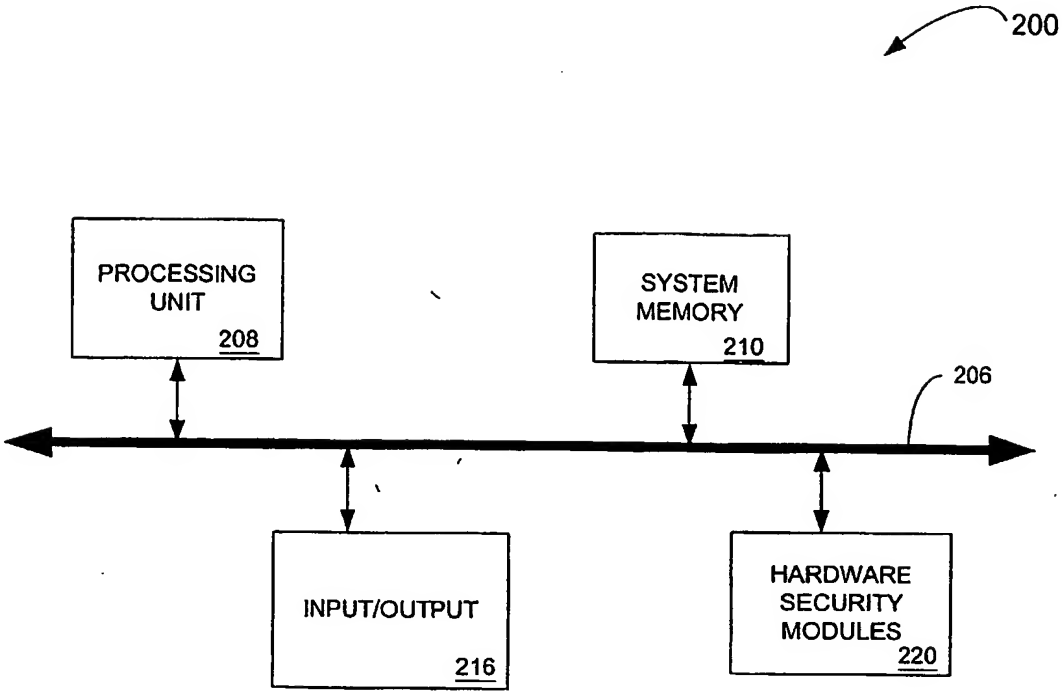
200
PROCESSING UNIT
208
SYSTEM MEMORY
210
206
INPUT/OUTPUT
216
HARDWARE SECURITY MODULES
220

FIG. 2

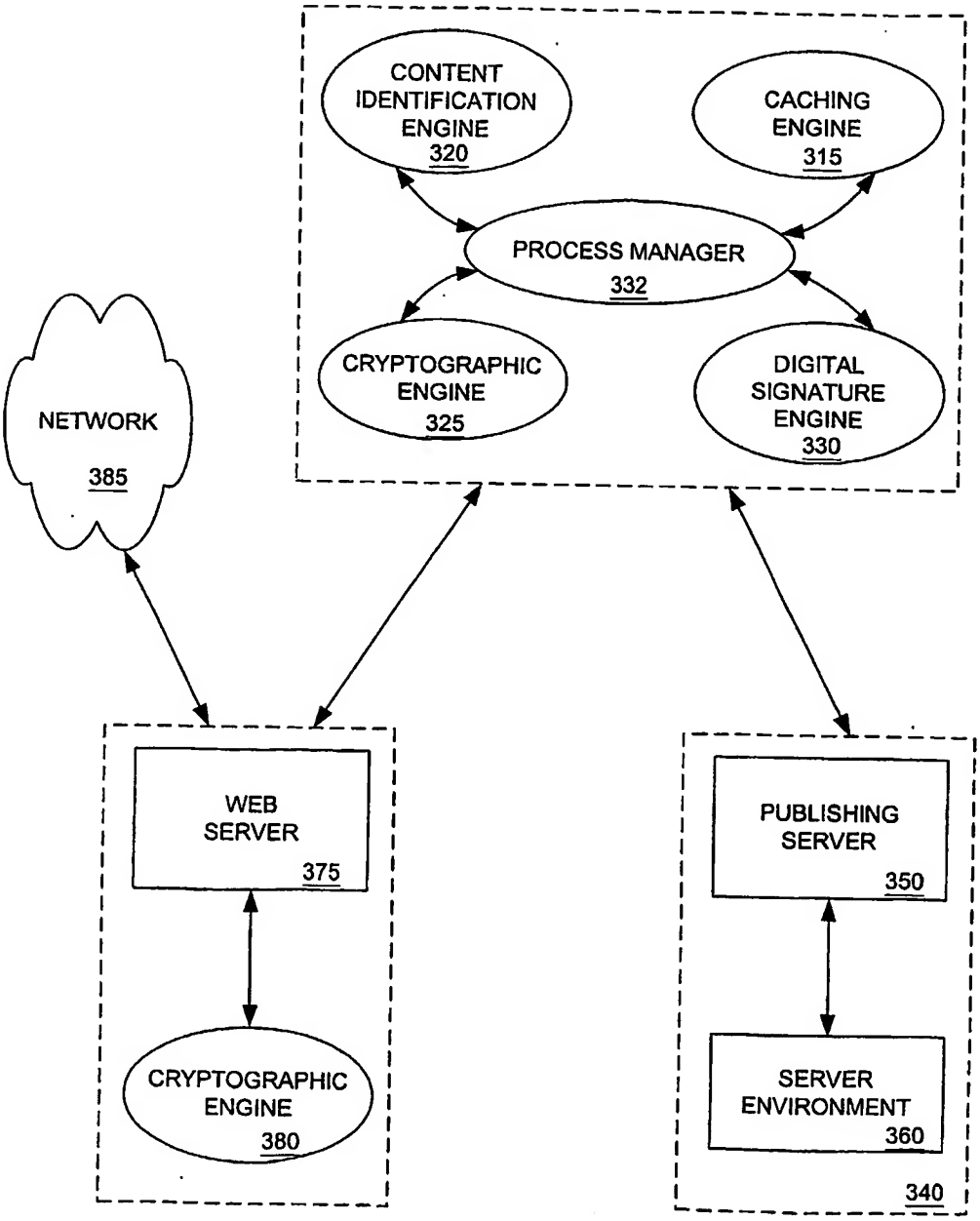
CONTENT IDENTIFICATION ENGINE 320
CACHING ENGINE 315
PROCESS MANAGER 332
CRYPTOGRAPHIC ENGINE 325
DIGITAL SIGNATURE ENGINE 330
NETWORK 385
WEB SERVER 375
CRYPTOGRAPHIC ENGINE 380
PUBLISHING SERVER 350
SERVER ENVIRONMENT 360
340

FIG. 3

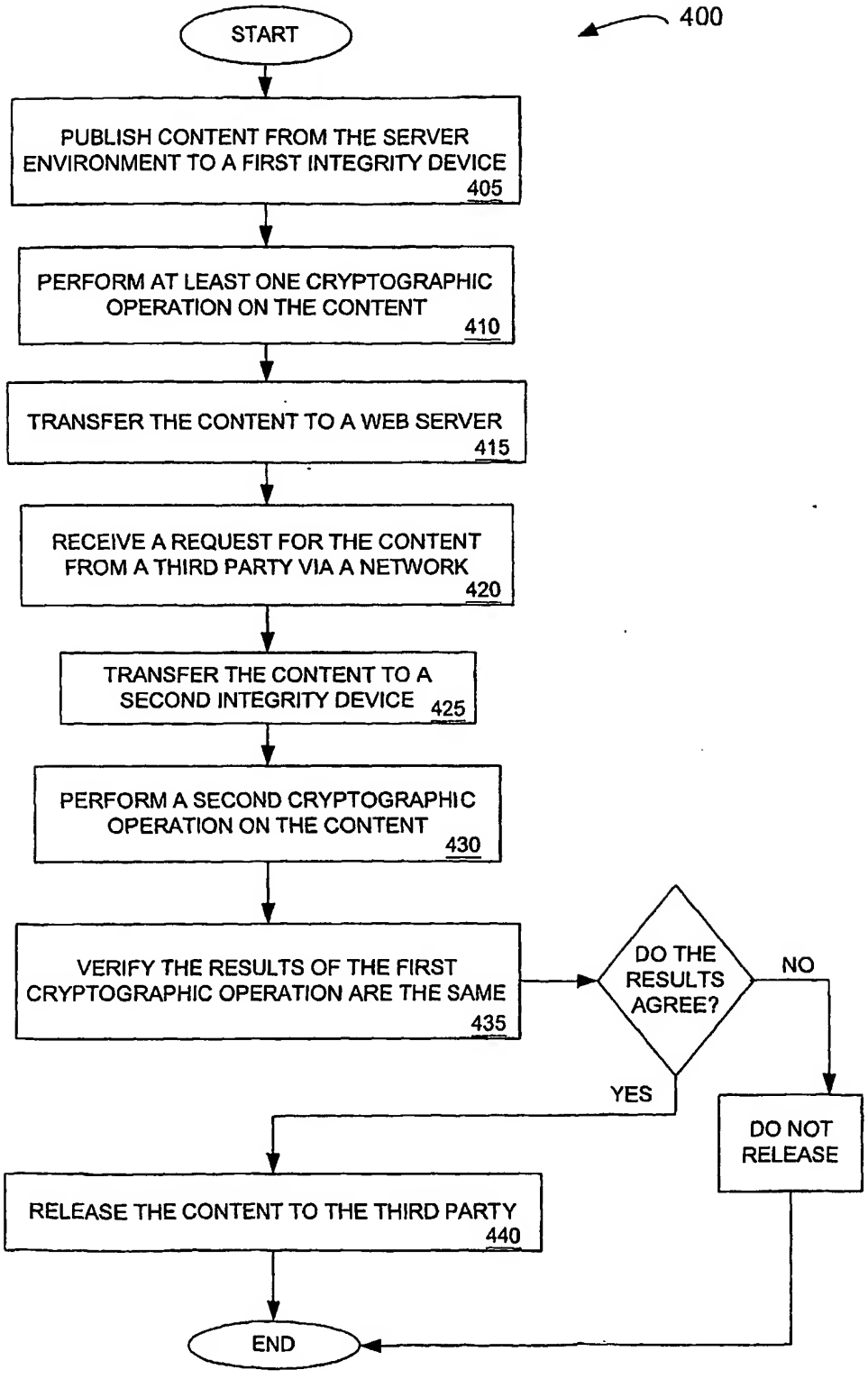
400
START
PUBLISH CONTENT FROM THE SERVER ENVIRONMENT TO A FIRST INTEGRITY DEVICE 405
PERFORM AT LEAST ONE CRYPTOGRAPHIC OPERATION ON THE CONTENT 410
TRANSFER THE CONTENT TO A WEB SERVER 415
RECEIVE A REQUEST FOR THE CONTENT FROM A THIRD PARTY VIA A NETWORK 420
TRANSFER THE CONTENT TO A SECOND INTEGRITY DEVICE 425
PERFORM A SECOND CRYPTOGRAPHIC OPERATION ON THE CONTENT 430
VERIFY THE RESULTS OF THE FIRST CRYPTOGRAPHIC OPERATION ARE THE SAME 435
DO THE RESULTS AGREE?
NO
YES
DO NOT RELEASE
RELEASE THE CONTENT TO THE THIRD PARTY 440
END

FIG. 4

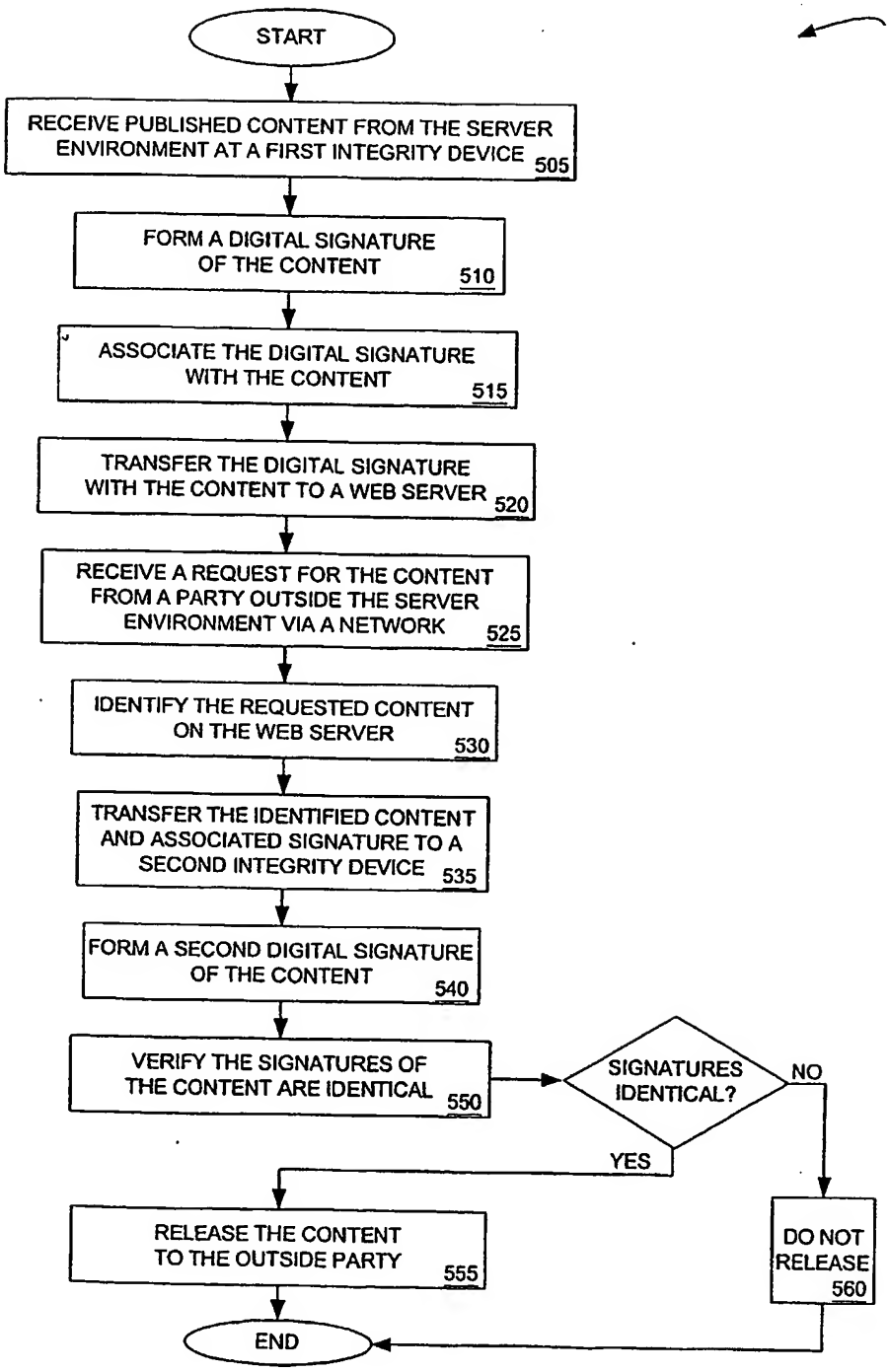
500
START
RECEIVE PUBLISHED CONTENT FROM THE SERVER ENVIRONMENT AT A FIRST INTEGRITY DEVICE 505
FORM A DIGITAL SIGNATURE OF THE CONTENT 510
ASSOCIATE THE DIGITAL SIGNATURE WITH THE CONTENT 515
TRANSFER THE DIGITAL SIGNATURE WITH THE CONTENT TO A WEB SERVER 520
RECEIVE A REQUEST FOR THE CONTENT FROM A PARTY OUTSIDE THE SERVER ENVIRONMENT VIA A NETWORK 525
IDENTIFY THE REQUESTED CONTENT ON THE WEB SERVER 530
TRANSFER THE IDENTIFIED CONTENT AND ASSOCIATED SIGNATURE TO A SECOND INTEGRITY DEVICE 535
FORM A SECOND DIGITAL SIGNATURE OF THE CONTENT 540
VERIFY THE SIGNATURES OF THE CONTENT ARE IDENTICAL 550
SIGNATURES IDENTICAL?
NO
YES
RELEASE THE CONTENT TO THE OUTSIDE PARTY 555
DO NOT RELEASE 560
END

FIG. 5

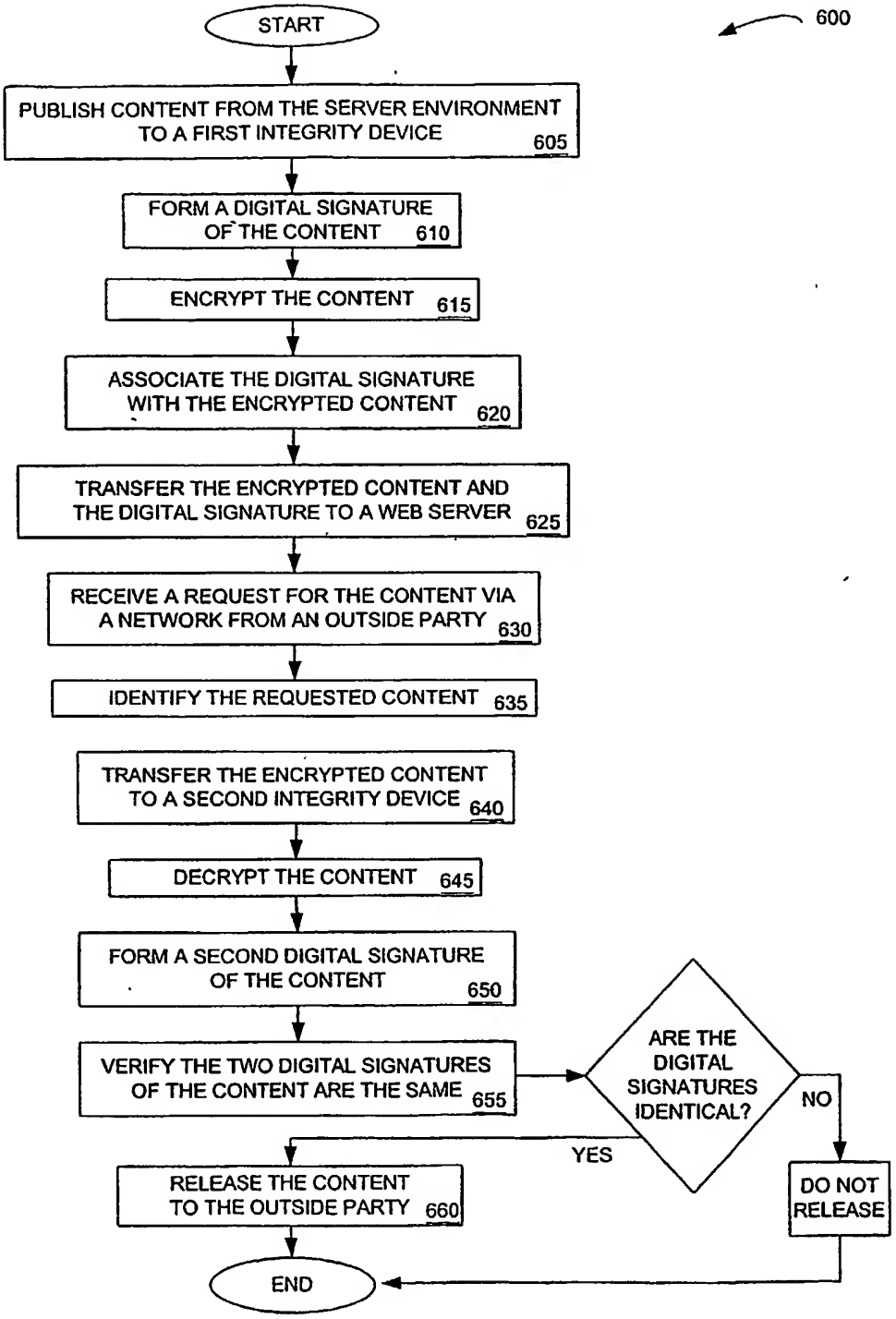
600
START
PUBLISH CONTENT FROM THE SERVER ENVIRONMENT TO A FIRST INTEGRITY DEVICE 605
FORM A DIGITAL SIGNATURE OF THE CONTENT 610
ENCRYPT THE CONTENT 615
ASSOCIATE THE DIGITAL SIGNATURE WITH THE ENCRYPTED CONTENT 620
TRANSFER THE ENCRYPTED CONTENT AND THE DIGITAL SIGNATURE TO A WEB SERVER 625
RECEIVE A REQUEST FOR THE CONTENT VIA A NETWORK FROM AN OUTSIDE PARTY 630
IDENTIFY THE REQUESTED CONTENT 635
TRANSFER THE ENCRYPTED CONTENT TO A SECOND INTEGRITY DEVICE 640
DECRYPT THE CONTENT 645
FORM A SECOND DIGITAL SIGNATURE OF THE CONTENT 650
VERIFY THE TWO DIGITAL SIGNATURES OF THE CONTENT ARE THE SAME 655
ARE THE DIGITAL SIGNATURES IDENTICAL?
NO
YES
RELEASE THE CONTENT TO THE OUTSIDE PARTY 660
DO NOT RELEASE
END

FIG. 6

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 03/03622

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F1/00 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HERDA S: "Non-repudiation: Constituting evidence and proof in digital cooperation" COMPUTER STANDARDS AND INTERFACES, ELSEVIER SEQUOIA. LAUSANNE, CH, vol. 17, no. 1, 1995, pages 69-79, XP004046750 ISSN: 0920-5489 page 70, right-hand column -page 71, right-hand column; figure 1 page 73, right-hand column -page 74, left-hand column; figure 2 --- -/--	1-76

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 June 2003	03/07/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern ıal Application No
PCT/US 03/03622

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	RSA LABORATORIES: "PKCS #7: Cryptographic Message Syntax Standard, Version 1.5" RSA LABORATORIES TECHNICAL NOTE, XX, XX, 1 November 1993 (1993-11-01), pages 1-30, XP002207635 page 1, paragraph 1 page 9 -page 10 -----	1-76

Form PCT/ISA/210 (continuation of second sheet) (July 1992)